What's new in Elastic Stack 7.x

Emanuil Tolev @emanuil_tolev

elastic

Community Engineer

Lots of things!

Search

Data management

Security

Search

Adaptive replica selection

Ever tried to load balance ES?

elastic

@emanuil_tolev

Skipping refreshes on idle shards

(wut?)

elastic

@emanuil_tolev

Default to 1 shard

Time for a tiny bit of theory

Cross-cluster search

Zen2

Quorum setting (`minimum_master_nodes`) gone!

Index Lifecycle Management is GA

elastic

@emanuil_tolev

```
PUT _ilm/policy/datastream_policy
{
  "policy": {
    "phases": {
      "hot": {
        "actions": {
          "rollover": {
            "max_size": "50GB",
            "max_age": "30d"
          }
        }
      },
      "delete": {
        "min_age": "90d",
        "actions": {
          "delete": {}
        }
      }
    }
  }
}
```

```
PUT _template/datastream_template
{
  "index_patterns": ["datastream-*"],
  "settings": {
    "number_of_shards": 1,
    "number_of_replicas": 1,
    "index.lifecycle.name": "datastream_policy",
    "index.lifecycle.rollover_alias": "datastream"
  }
}
```

```
PUT datastream-000001
{
  "aliases": {
    "datastream": {
      "is_write_index": true
    }
  }
}
```

```
GET datastream-*/_ilm/explain

// aaaand:
{
  "indices": {
    "datastream-000001": {
      "index": "datastream-000001",
      "managed": true,
      "policy": "datastream_policy",
      "phase": "hot",                    <-- 1
      "action": "rollover",              <-- 2
      "step": "attempt-rollover",        <-- 3
      "phase_execution": {
        "policy": "datastream_policy",
        "phase_definition": {
          // ... 50 GB or max age 30 days, etc.
          }
        }
      }
    }
  }
}
```

"datastream": alias for searching and writing

SQL is now GA

How to use it?

→ the usual REST endpoints

→ the ES SQL command line interface

→ the JDBC driver

→ the ODBC driver

```
POST /_sql?format=txt
{
    "query": "SELECT * FROM library ORDER BY page_count DESC LIMIT 5"
}
```

```
author      |        name         |  page_count   | release_date
----------------+---------------------+---------------+------------------------
Peter F. Hamilton|Pandora's Star      |768            |2004-03-02T00:00:00.000Z
Vernor Vinge    |A Fire Upon the Deep|613            |1992-06-01T00:00:00.000Z
Frank Herbert   |Dune                |604            |1965-06-01T00:00:00.000Z
Alastair Reynolds|Revelation Space   |585            |2000-03-15T00:00:00.000Z
James S.A. Corey |Leviathan Wakes    |561            |2011-06-02T00:00:00.000Z
```

```
$ ./bin/elasticsearch-sql-cli https://sql_user:strongpassword@some.server:9200

sql> SELECT * FROM library WHERE page_count > 500 ORDER BY page_count DESC;
     author      |        name         |  page_count   | release_date
-----------------+---------------------+---------------+---------------
Peter F. Hamilton|Pandora's Star       |768            |1078185600000
Vernor Vinge     |A Fire Upon the Deep|613            |707356800000
Frank Herbert    |Dune                 |604            |-144720000000
Alastair Reynolds|Revelation Space     |585            |953078400000
James S.A. Corey |Leviathan Wakes      |561            |1306972800000
```

Data frames

In the spirit of connecting with nostalgia, basically pivot tables

Summarise one index into another one

Search as you type field type

`search_as_you_type` **in the mapping**

Flattened field type

`flattened` in the mapping

elastic

@emanuil_tolev

Rare terms agg

`"order" : { "_count" : "asc" }` **on a Terms agg**

JSON logging

elastic

@emanuil_tolev

vector similarity search

elastic

@emanuil_tolev

TLS intra-cluster encryption now free

elastic

@emanuil_tolev

RBAC (Role Based Access Control) also free

a free SIEM

elastic

@emanuil_tolev

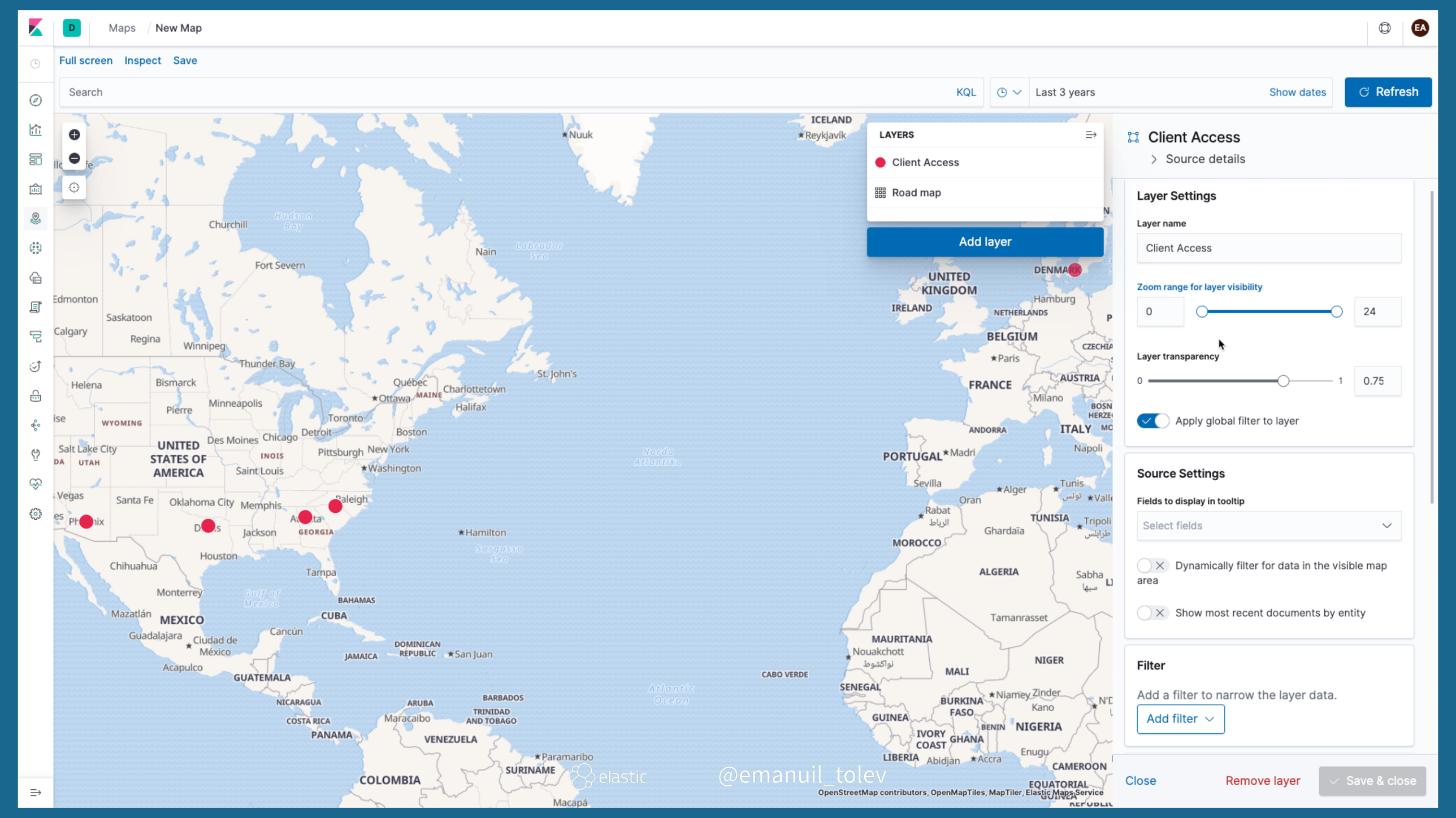
APM

.NET is now GA

Interesting maps integration for the JS Real User Monitoring (RUM)

elastic

@emanuil_tolev


Maps / New Map
Full screen
Inspect
Save
Search
KQL
Last 3 years
Show dates
Refresh
LAYERS
Client Access
Road map
Add layer
Client Access
Source details
Layer Settings
Layer name
Client Access
Zoom range for layer visibility
0
24
Layer transparency
0
1
0.75
Apply global filter to layer
Source Settings
Fields to display in tooltip
Select fields
Dynamically filter for data in the visible map area
Show most recent documents by entity
Filter
Add a filter to narrow the layer data.
Add filter
Close
Remove layer
Save & close
@emanuil_tolev
OpenStreetMap contributors, OpenMapTiles, MapTiler, Elastic Maps Service

Manchester!

GOVERNMENT DAY on Wed September 11, 9am until 5pm

https://events.elastic.co/2019911elasticgovernmentday

KUBERNETES WORKSHOP on Thu September 12, 9am until 1pm

http://events.elastic.co/2019912monitoringkubernetes

More free educational events for Manchester

Manchester is a priority city. Looking at **ML, security, on top of Logging, APM, Observability**

→ Host, speak or just stay informed: genevieve.loriant@elastic.co or me, etolev@elastic.co

→ BBLs!

Questions?

Emanuil Tolev @emanuil_tolev

etolev@elastic.co